FIG. 1

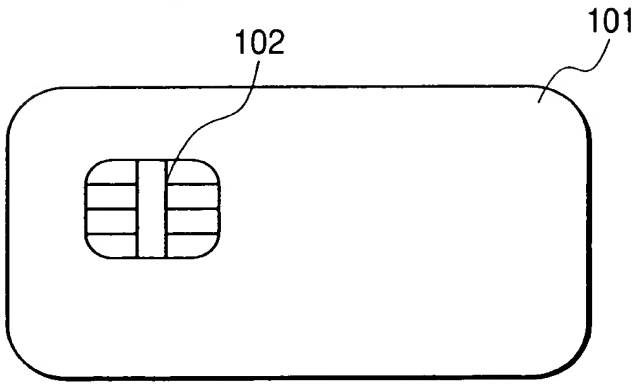

102
101

FIG. 2

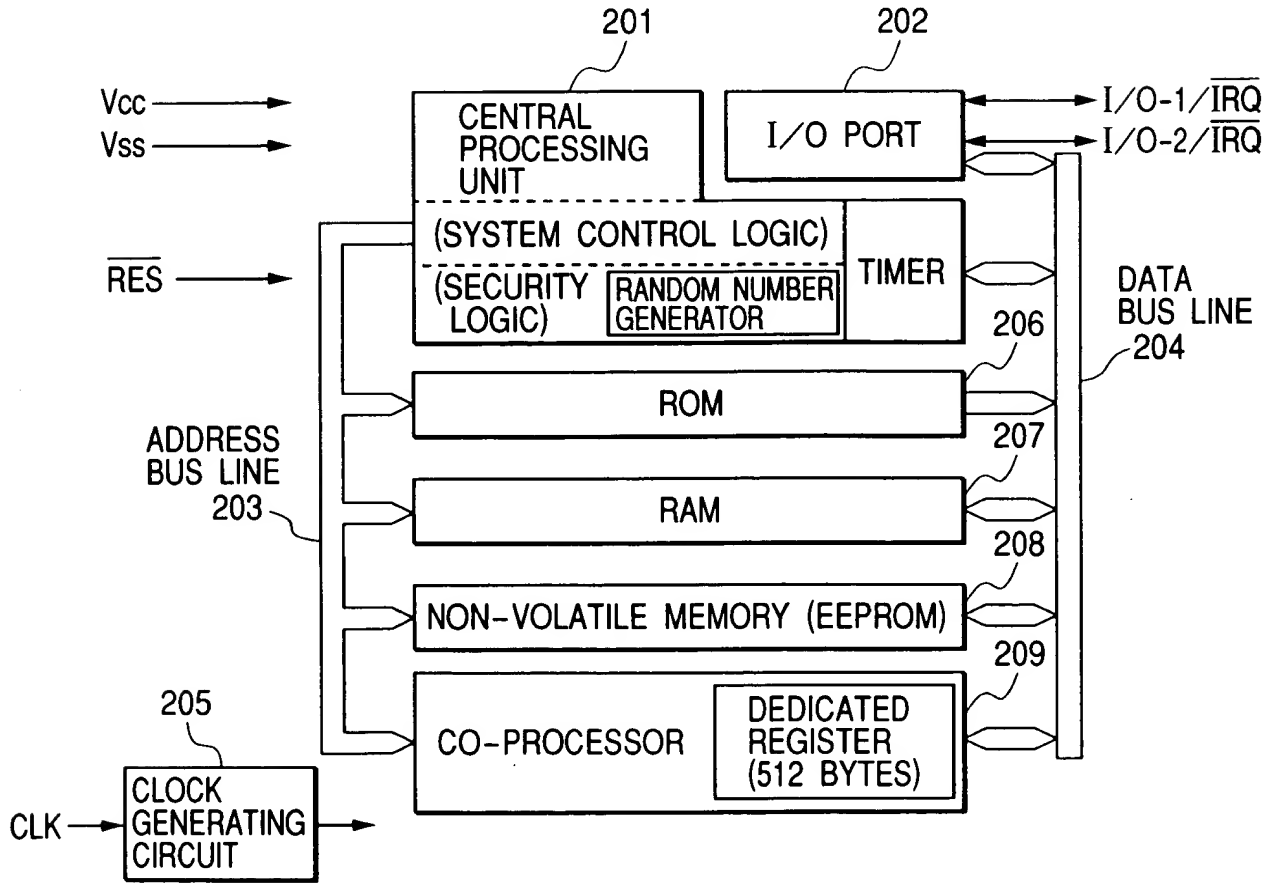

201
202
Vcc
Vss
CENTRAL PROCESSING UNIT
I/O PORT
I/O-1/IRQ
I/O-2/IRQ
(SYSTEM CONTROL LOGIC)
RES
(SECURITY LOGIC)
RANDOM NUMBER GENERATOR
TIMER
DATA BUS LINE
204
206
ROM
ADDRESS BUS LINE
203
207
RAM
208
NON-VOLATILE MEMORY (EEPROM)
209
205
CO-PROCESSOR
DEDICATED REGISTER (512 BYTES)
CLK
CLOCK GENERATING CIRCUIT

FIG. 3(a)

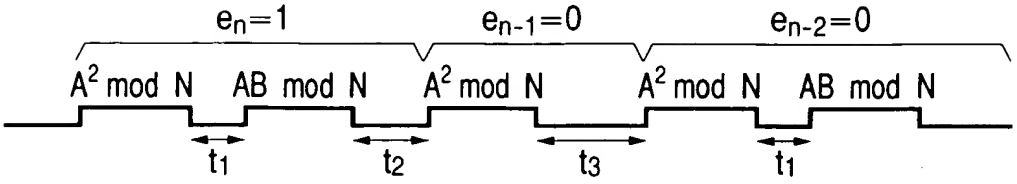


FIG. 3(b)

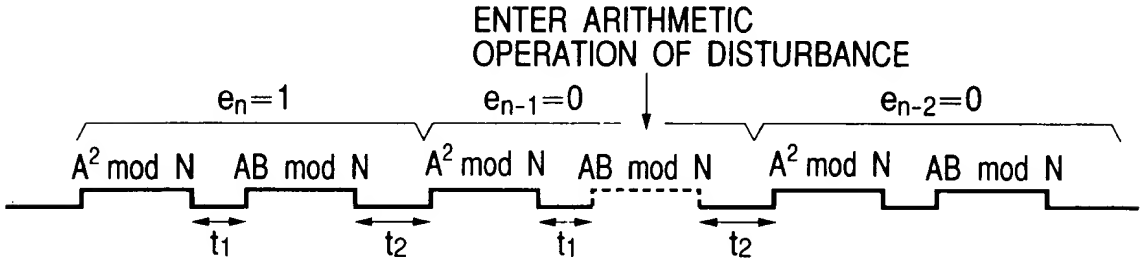


FIG. 4

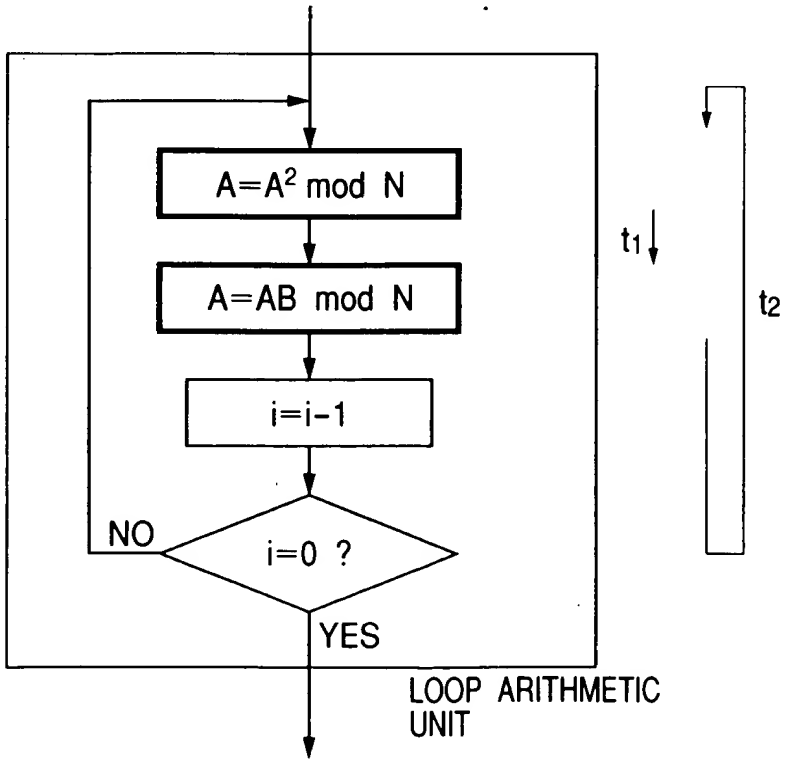


FIG. 5

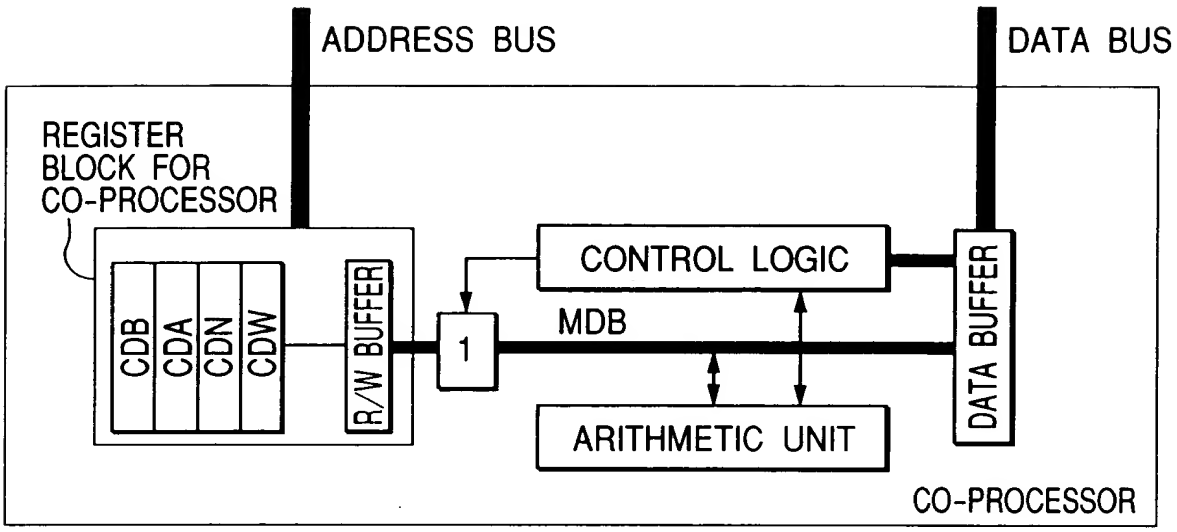

ADDRESS BUS
DATA BUS
REGISTER BLOCK FOR CO-PROCESSOR
CDB
CDA
CDN
CDW
R/W BUFFER
1
CONTROL LOGIC
MDB
DATA BUFFER
ARITHMETIC UNIT
CO-PROCESSOR

FIG. 6

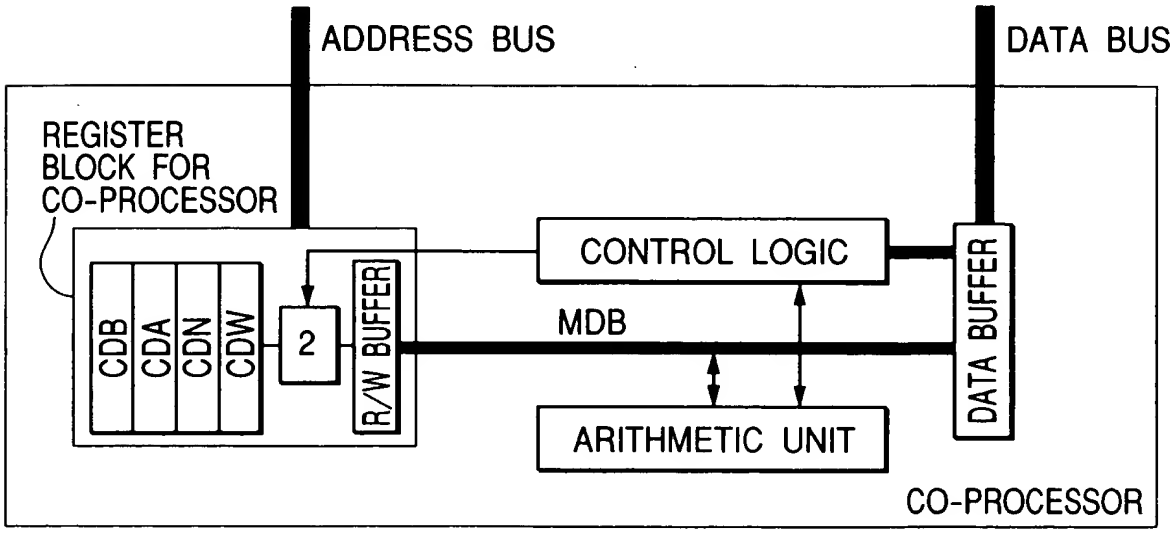

ADDRESS BUS
DATA BUS
REGISTER BLOCK FOR CO-PROCESSOR
CDB
CDA
CDN
CDW
2
R/W BUFFER
CONTROL LOGIC
MDB
DATA BUFFER
ARITHMETIC UNIT
CO-PROCESSOR

FIG. 7

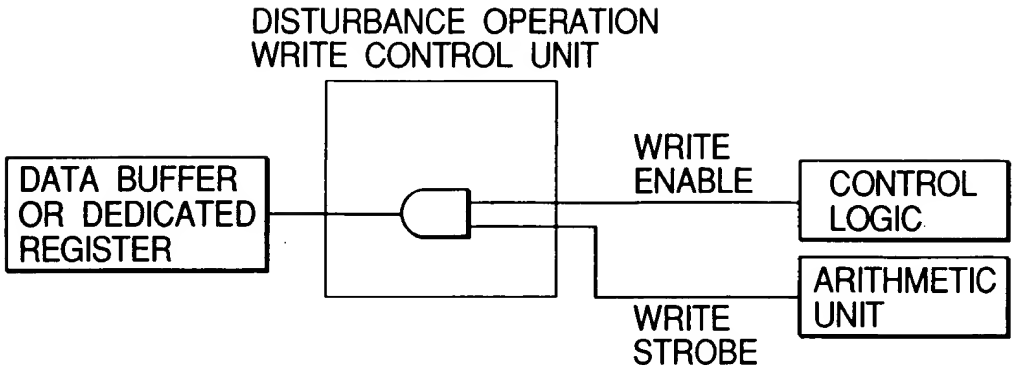

DISTURBANCE OPERATION
WRITE CONTROL UNIT
DATA BUFFER
OR DEDICATED
REGISTER
WRITE
ENABLE
CONTROL
LOGIC
ARITHMETIC
UNIT
WRITE
STROBE

FIG. 8

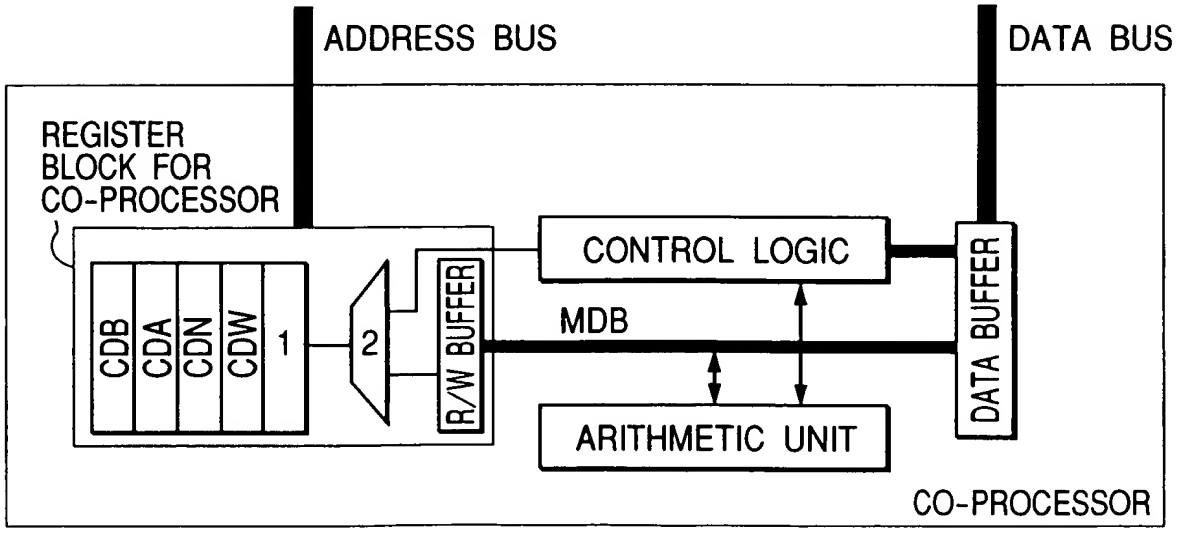

ADDRESS BUS
DATA BUS
REGISTER
BLOCK FOR
CO-PROCESSOR
CDB
CDA
CDN
CDW
1
2
R/W BUFFER
CONTROL LOGIC
MDB
DATA BUFFER
ARITHMETIC UNIT
CO-PROCESSOR

FIG. 9(a)

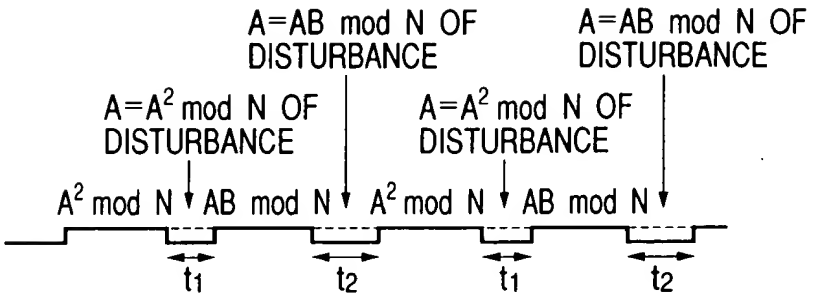


FIG. 9(b)

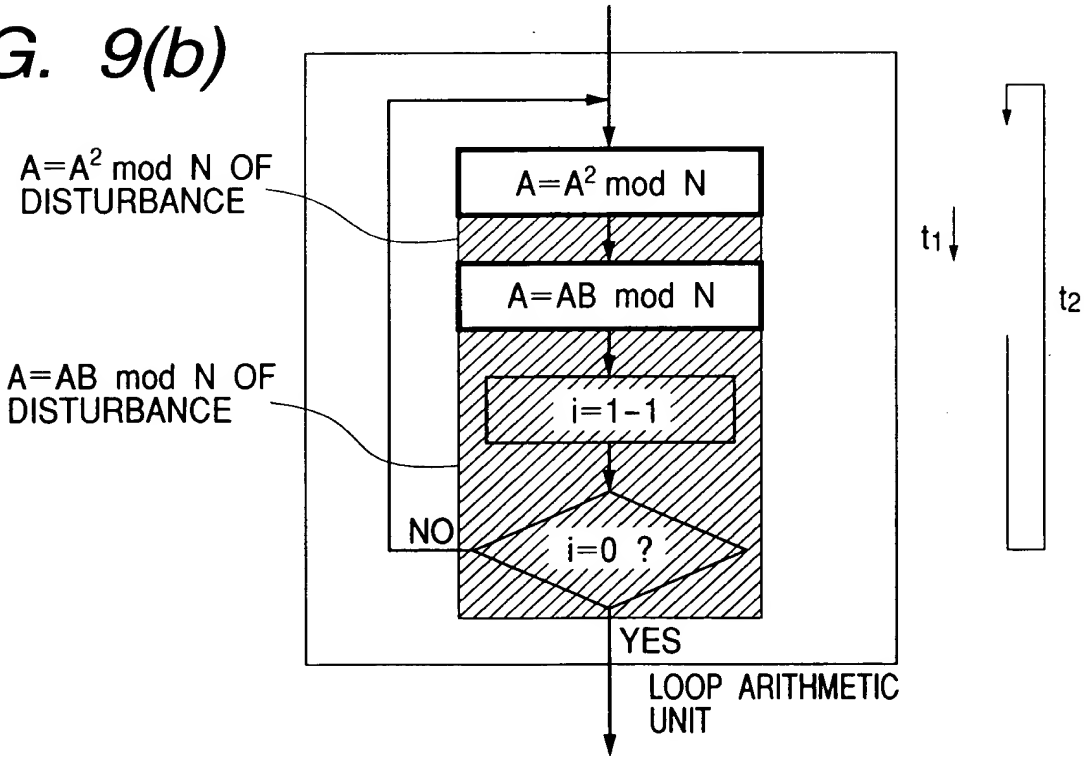


FIG. 10

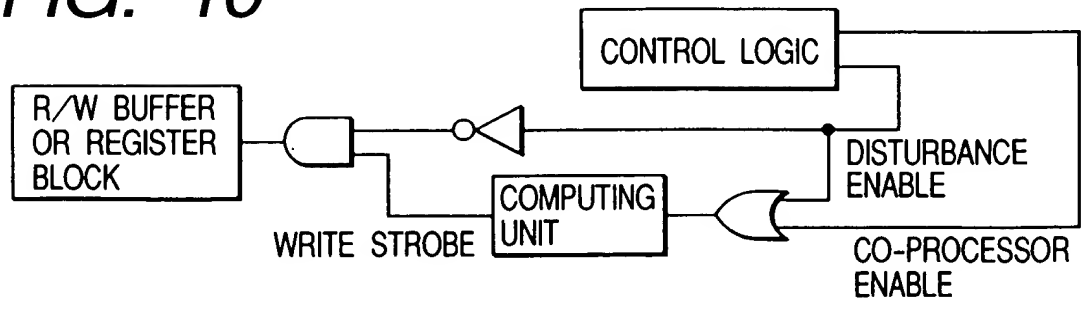


FIG. 11(a)

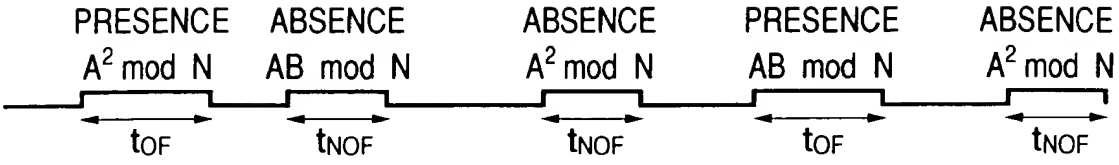


FIG. 11(b)

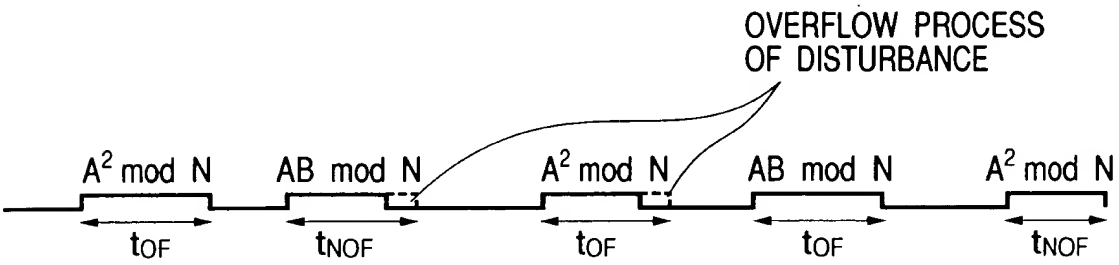


FIG. 12

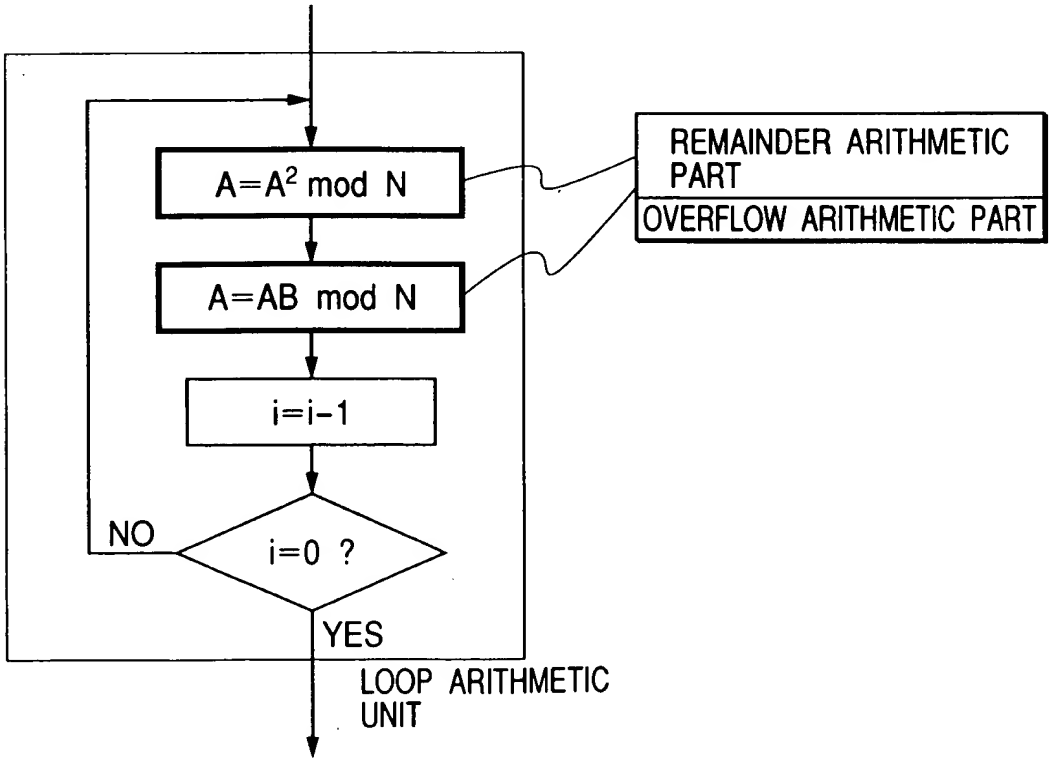


FIG. 13(a)

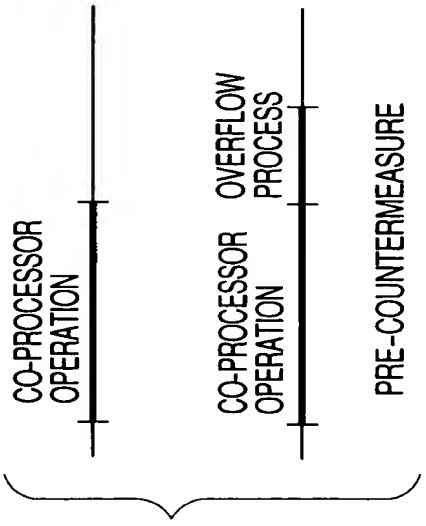


FIG. 13(b)

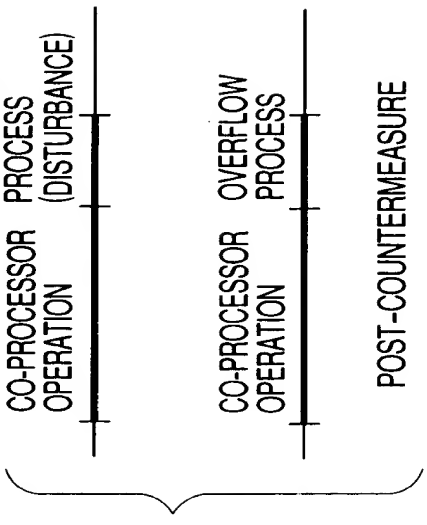
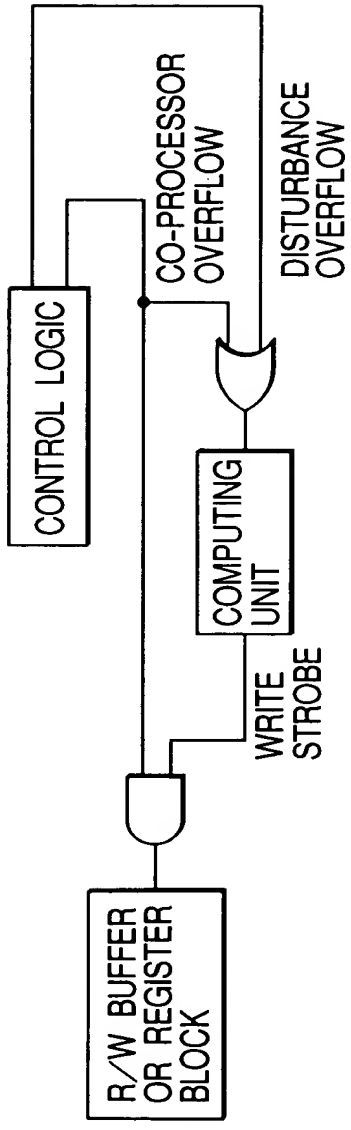


FIG. 14



PCT/JP2003/000000

FIG. 15(a)

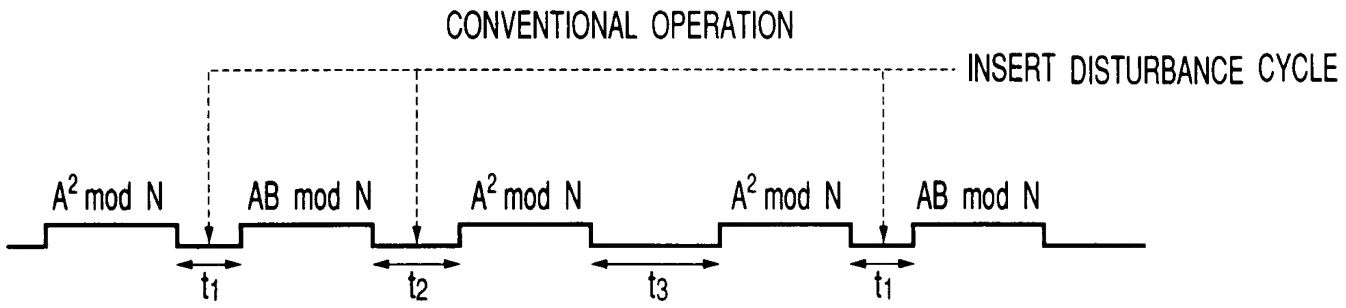


FIG. 15(b)

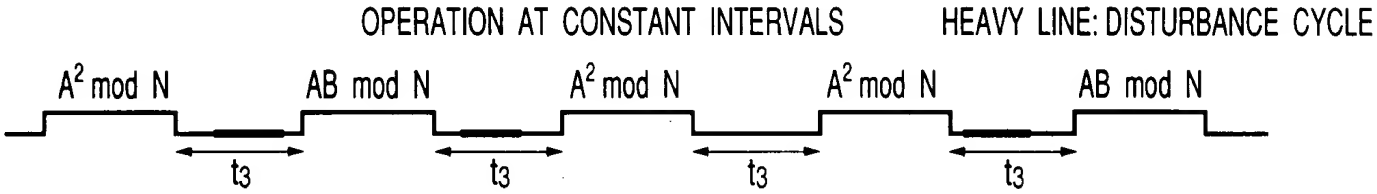


FIG. 15(c)

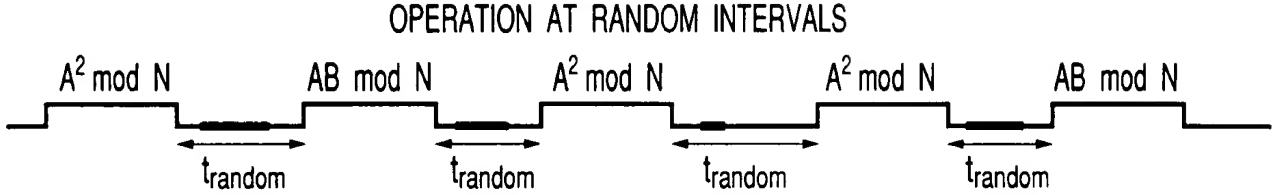


FIG. 16

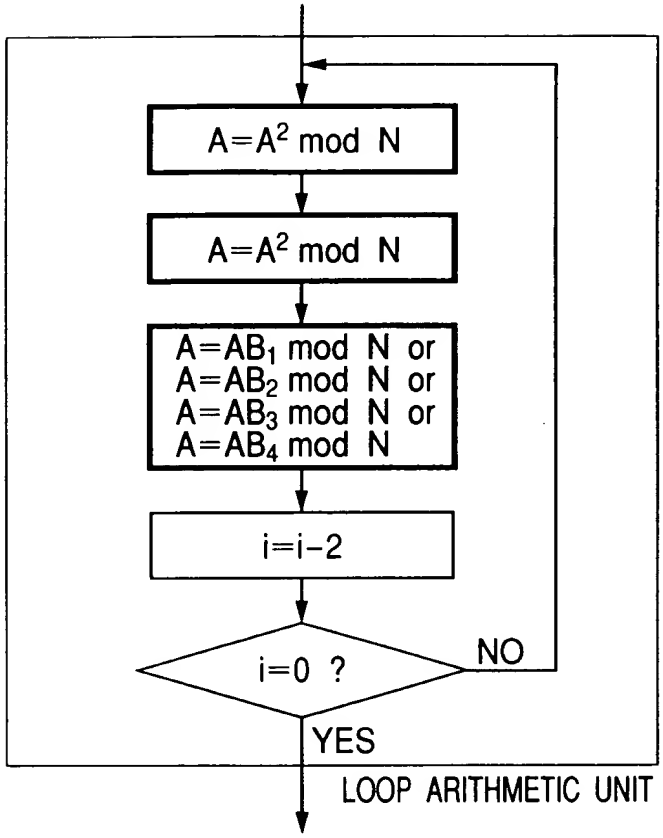

A=A² mod N
A=A² mod N
A=AB1 mod N or
A=AB2 mod N or
A=AB3 mod N or
A=AB4 mod N
i=i-2
i=0 ?
NO
YES
LOOP ARITHMETIC UNIT

FIG. 17

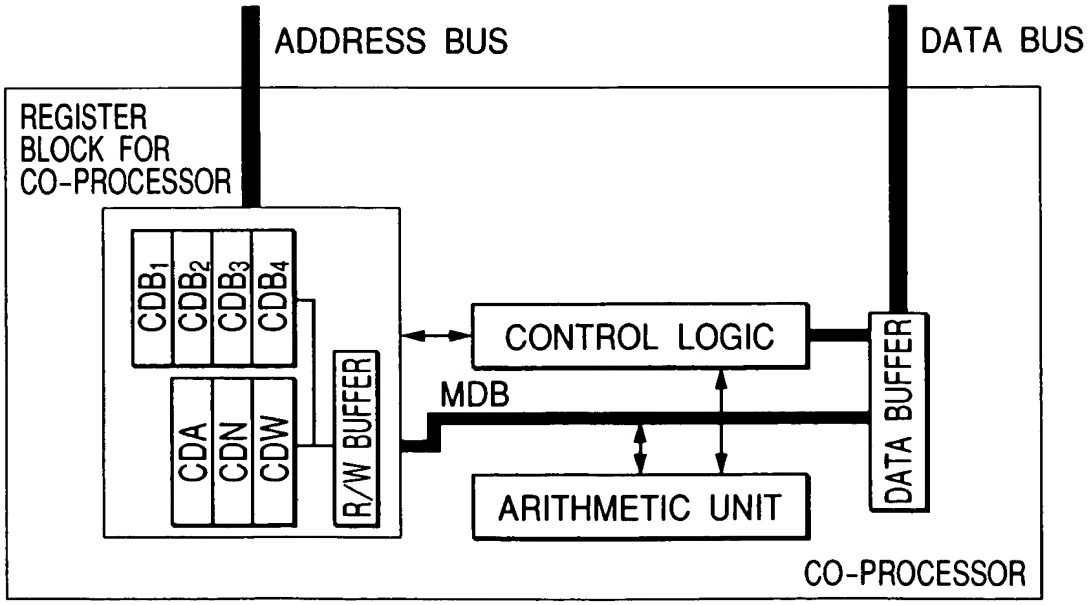

ADDRESS BUS
DATA BUS
REGISTER BLOCK FOR CO-PROCESSOR
CDB1
CDB2
CDB3
CDB4
CDA
CDN
CDW
R/W BUFFER
CONTROL LOGIC
MDB
DATA BUFFER
ARITHMETIC UNIT
CO-PROCESSOR

FIG. 18

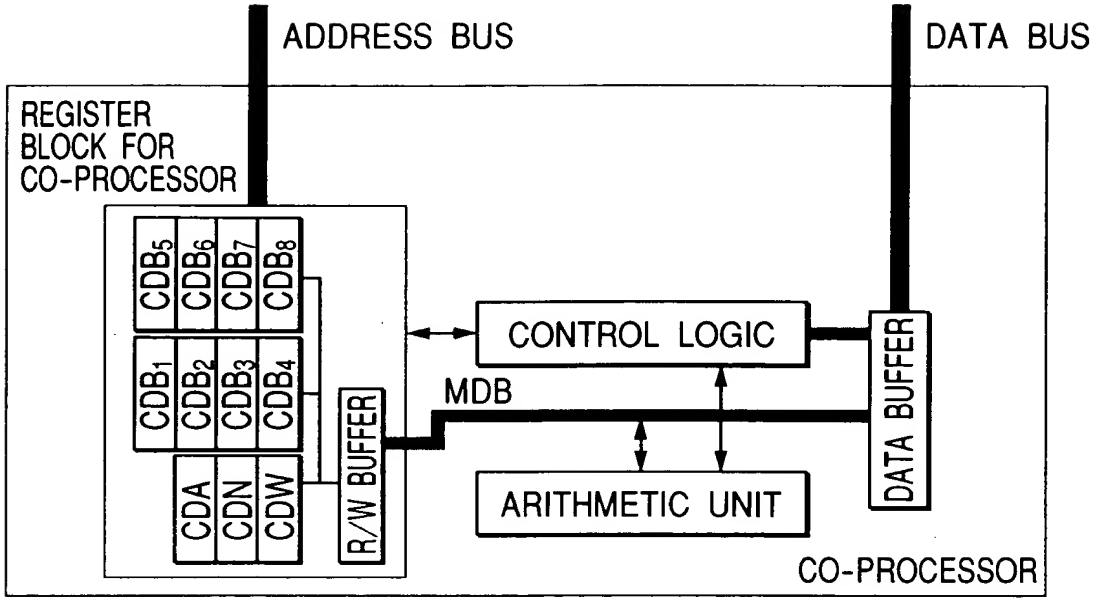

ADDRESS BUS
DATA BUS
REGISTER BLOCK FOR CO-PROCESSOR
CDB5
CDB6
CDB7
CDB8
CDB1
CDB2
CDB3
CDB4
CDA
CDN
CDW
R/W BUFFER
CONTROL LOGIC
MDB
ARITHMETIC UNIT
DATA BUFFER
CO-PROCESSOR

FIG. 19

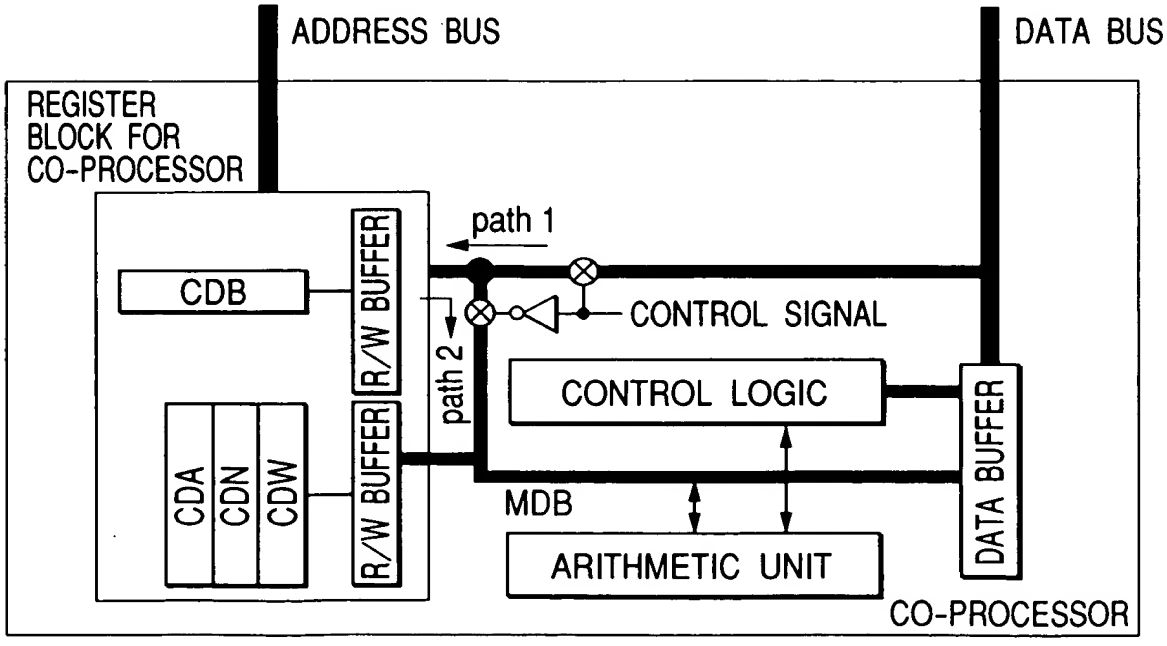

ADDRESS BUS
DATA BUS
REGISTER BLOCK FOR CO-PROCESSOR
path 1
CDB
R/W BUFFER
CONTROL SIGNAL
path 2
CONTROL LOGIC
CDA
CDN
CDW
R/W BUFFER
MDB
DATA BUFFER
ARITHMETIC UNIT
CO-PROCESSOR

FIG. 20

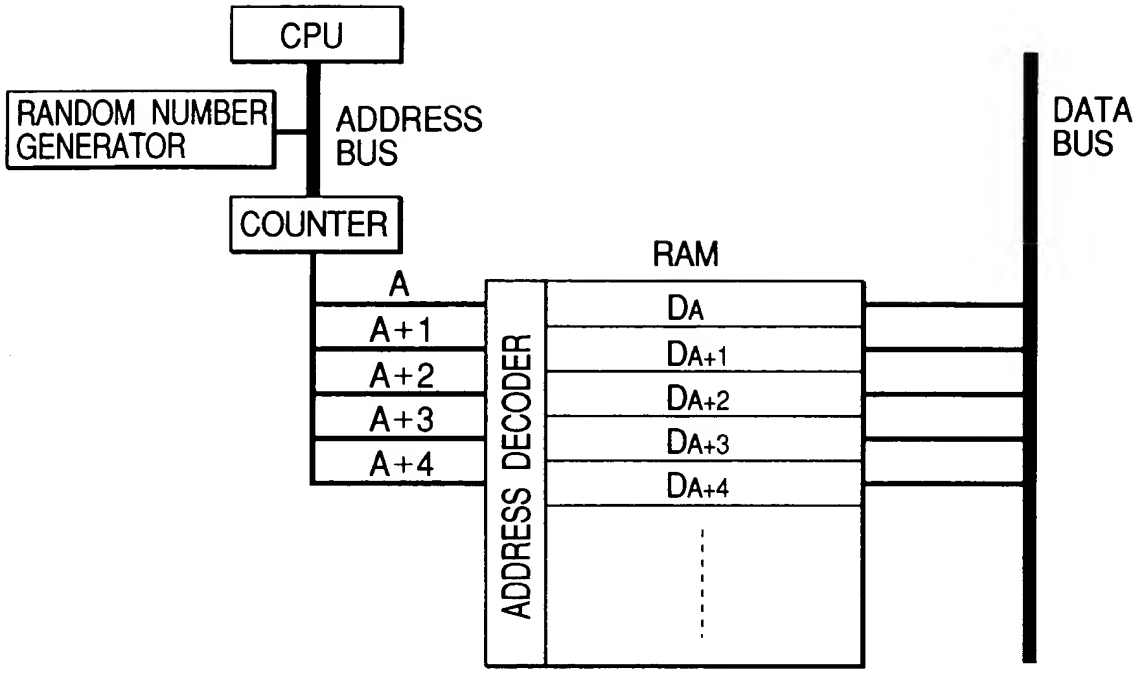

CPU
RANDOM NUMBER GENERATOR
ADDRESS BUS
COUNTER
DATA BUS
RAM
A
A+1
A+2
A+3
A+4
ADDRESS DECODER
DA
DA+1
DA+2
DA+3
DA+4

FIG. 21

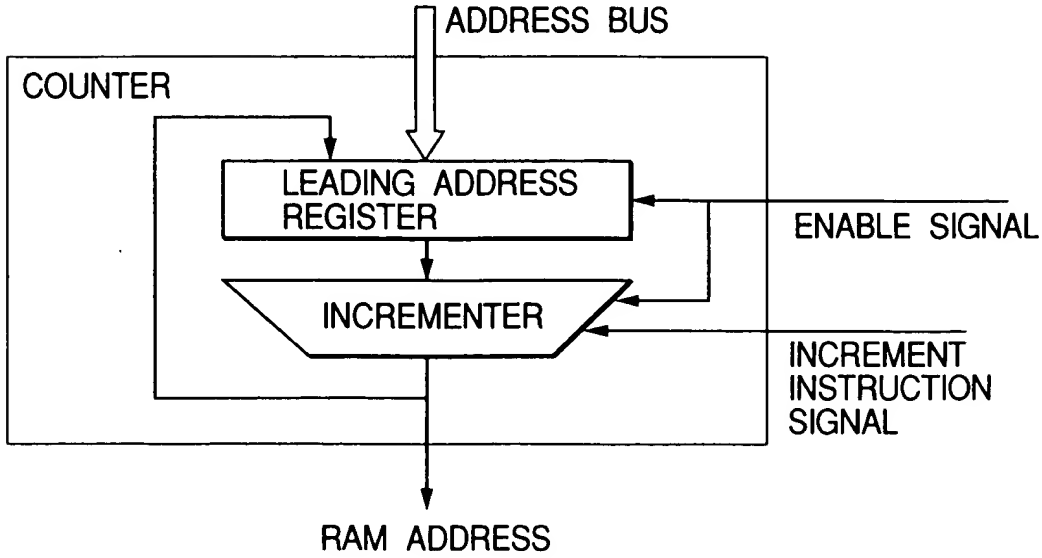

ADDRESS BUS
COUNTER
LEADING ADDRESS REGISTER
ENABLE SIGNAL
INCREMENTER
INCREMENT INSTRUCTION SIGNAL
RAM ADDRESS

FIG. 22

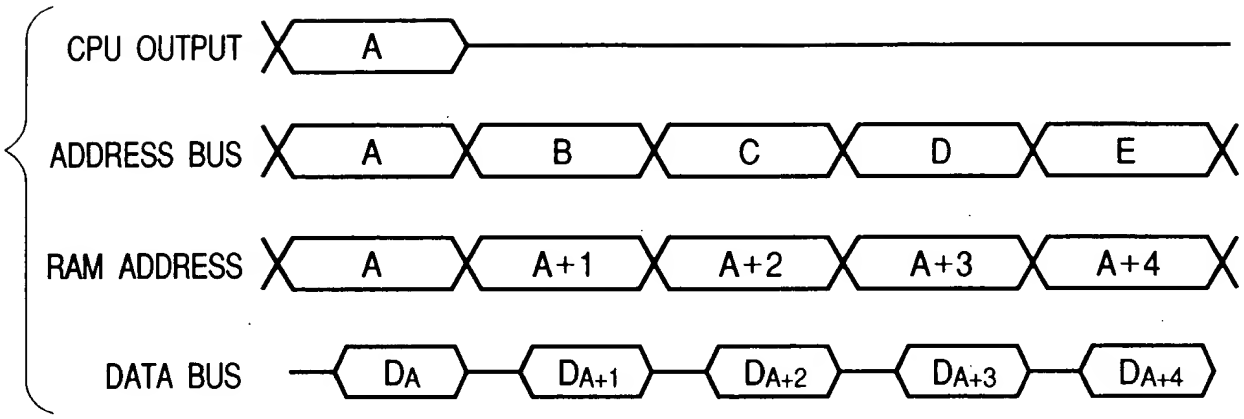

CPU OUTPUT
A
ADDRESS BUS
A
B
C
D
E
RAM ADDRESS
A
A+1
A+2
A+3
A+4
DATA BUS
DA
DA+1
DA+2
DA+3
DA+4

FIG. 23

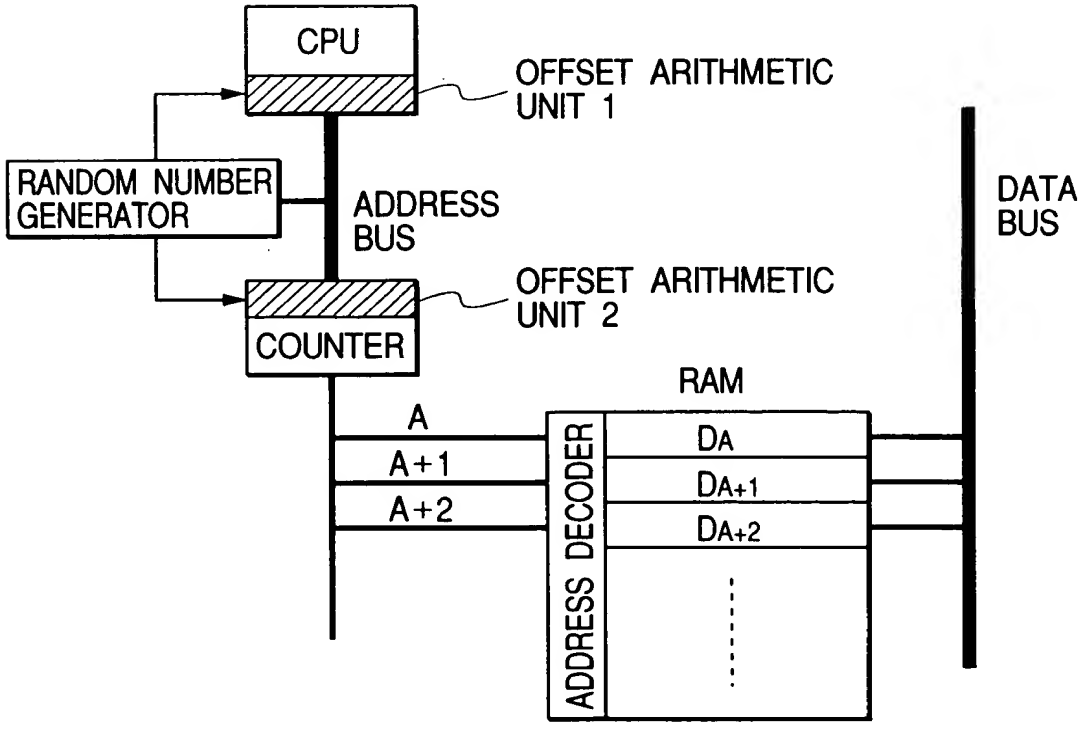

CPU
OFFSET ARITHMETIC UNIT 1
RANDOM NUMBER GENERATOR
ADDRESS BUS
DATA BUS
OFFSET ARITHMETIC UNIT 2
COUNTER
RAM
A
A+1
A+2
ADDRESS DECODER
DA
DA+1
DA+2

FIG. 24

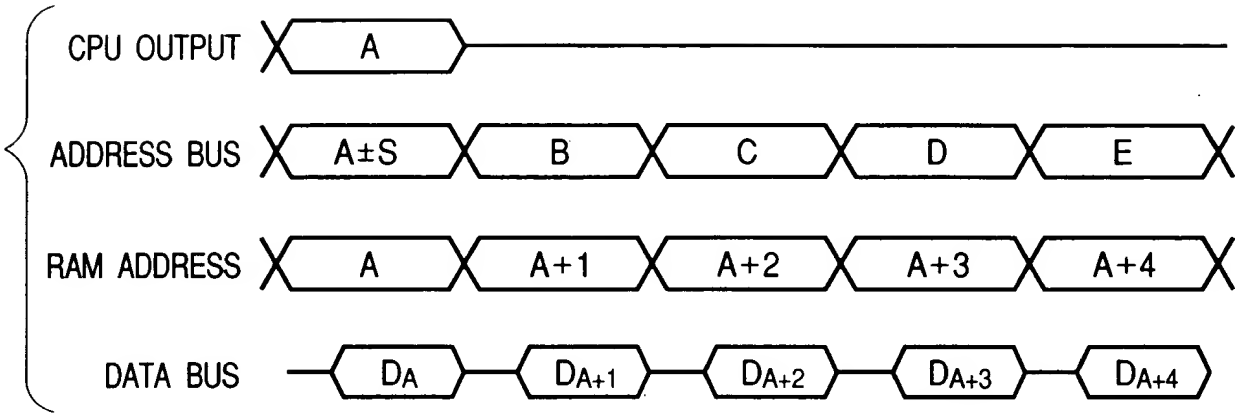

CPU OUTPUT
A
ADDRESS BUS
A±S
B
C
D
E
RAM ADDRESS
A
A+1
A+2
A+3
A+4
DATA BUS
DA
DA+1
DA+2
DA+3
DA+4

FIG. 26

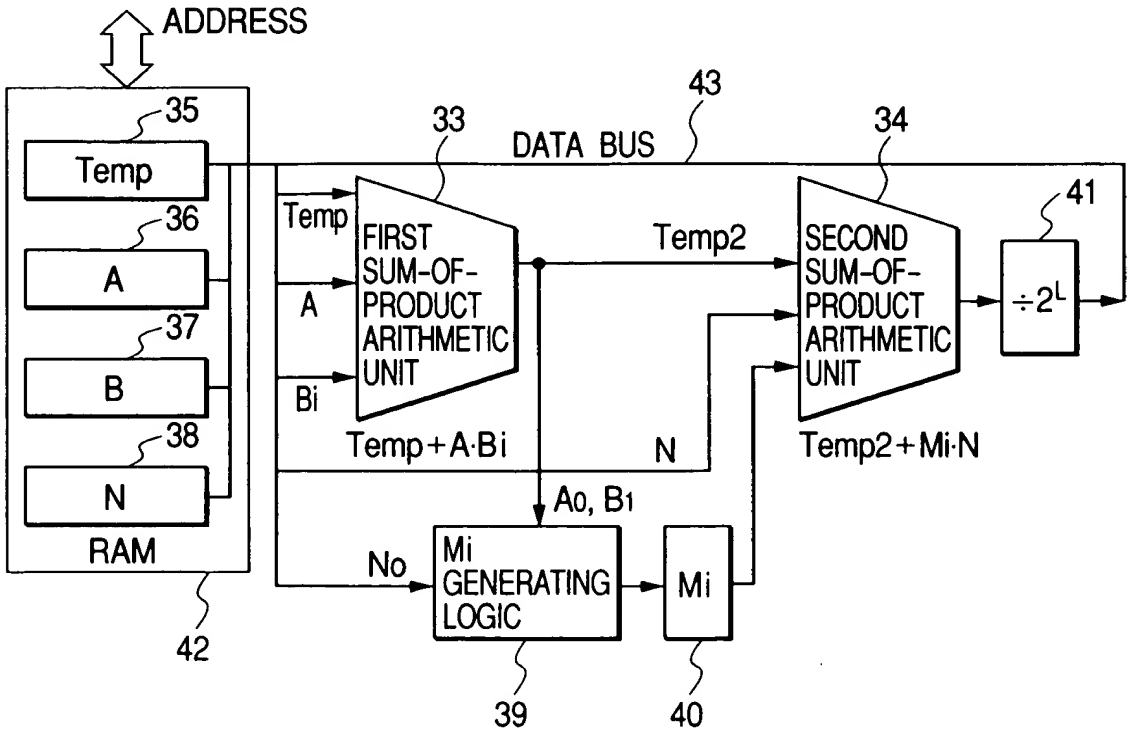

ADDRESS
35
Temp
36
A
37
B
38
N
RAM
42
33
43
DATA BUS
34
41
Temp
A
Bi
FIRST SUM-OF-PRODUCT ARITHMETIC UNIT
Temp+A·Bi
Temp2
SECOND SUM-OF-PRODUCT ARITHMETIC UNIT
÷2L
Temp2+Mi·N
N
Ao, B1
No
Mi GENERATING LOGIC
39
Mi
40

FIG. 25

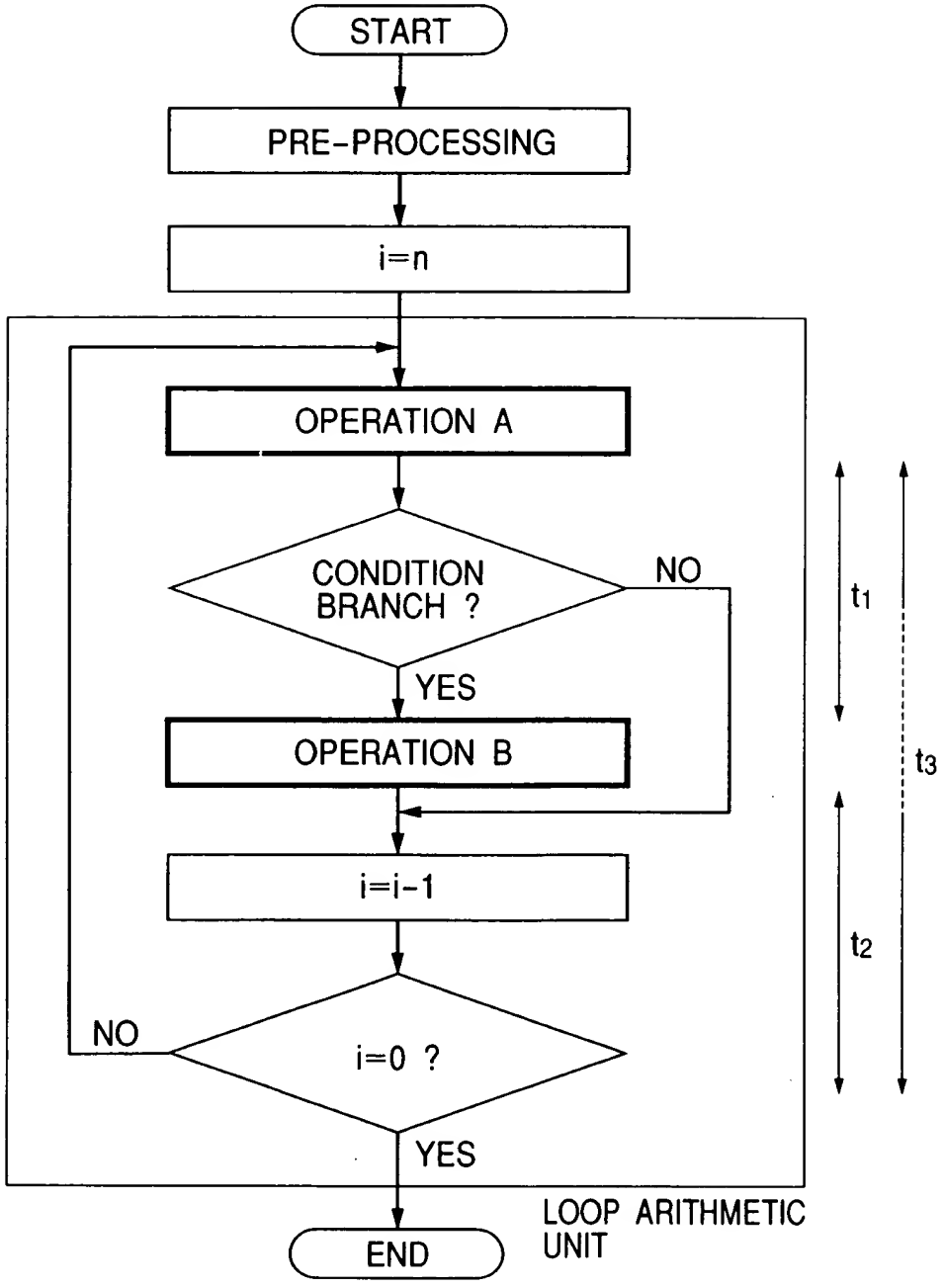

START
PRE-PROCESSING
i=n
OPERATION A
CONDITION BRANCH ?
NO
YES
OPERATION B
i=i-1
i=0 ?
NO
YES
END
LOOP ARITHMETIC UNIT
t1
t2
t3

FIG. 27

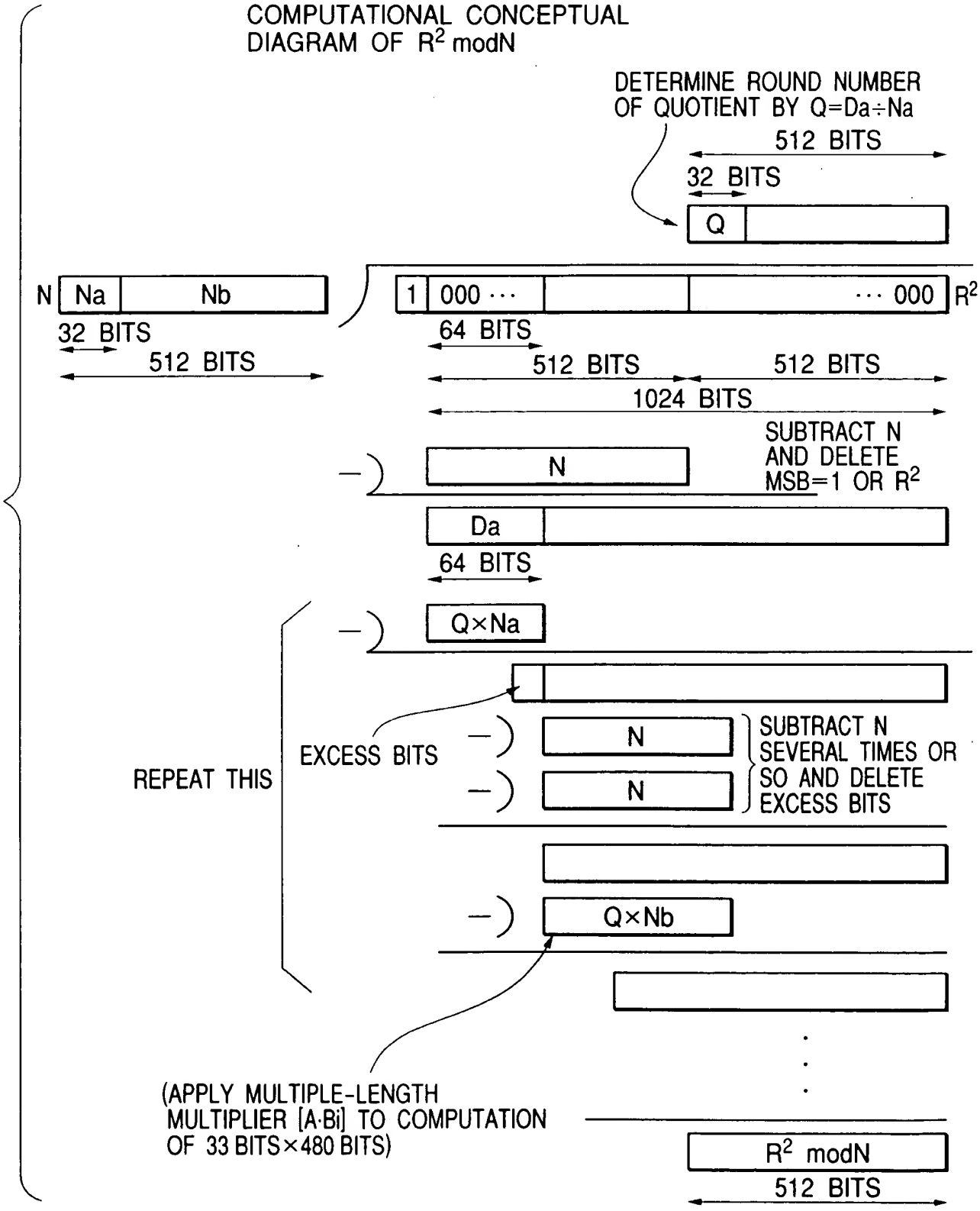

COMPUTATIONAL CONCEPTUAL DIAGRAM OF R^2 modN
DETERMINE ROUND NUMBER OF QUOTIENT BY Q=Da÷Na
512 BITS
32 BITS
Q
N
Na
Nb
32 BITS
512 BITS
1
000 ···
··· 000
R^2
64 BITS
512 BITS
512 BITS
1024 BITS
SUBTRACT N AND DELETE MSB=1 OR R^2
N
Da
64 BITS
Q×Na
REPEAT THIS
EXCESS BITS
N
N
SUBTRACT N SEVERAL TIMES OR SO AND DELETE EXCESS BITS
Q×Nb
(APPLY MULTIPLE-LENGTH MULTIPLIER [A·Bi] TO COMPUTATION OF 33 BITS×480 BITS)
R^2 modN
512 BITS

FIG. 28

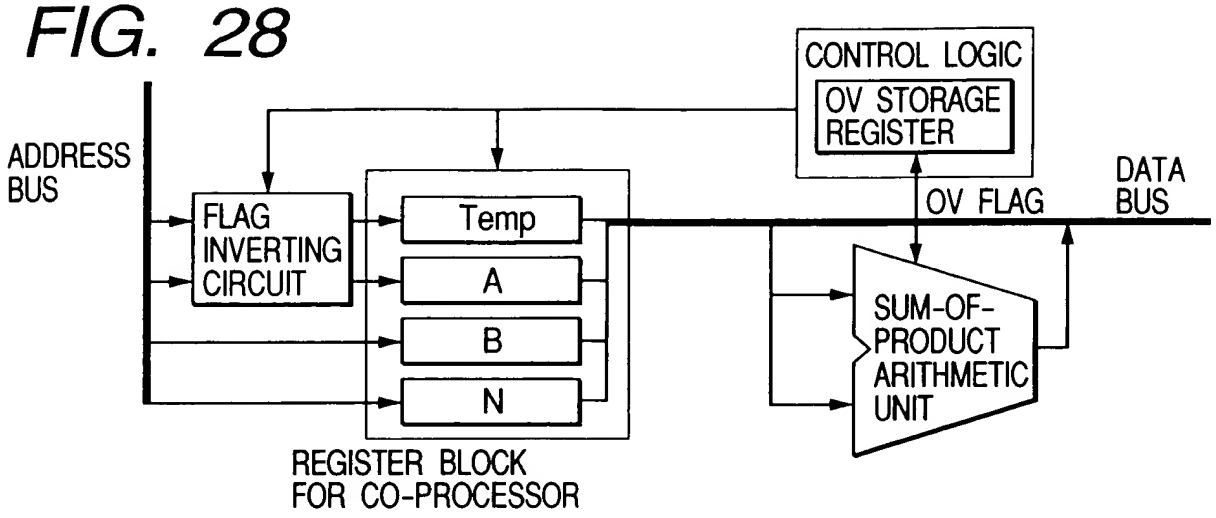


FIG. 29

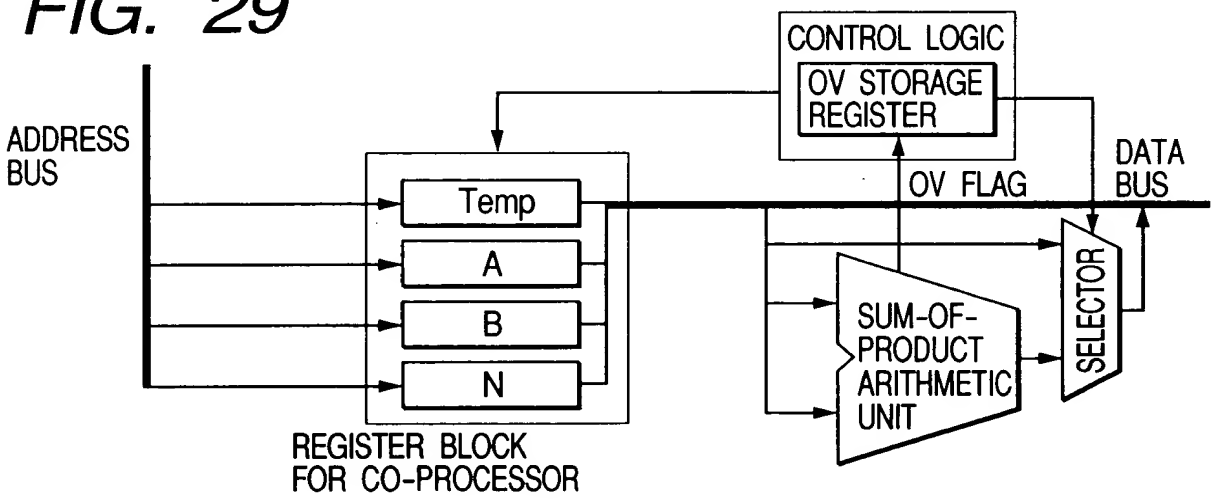
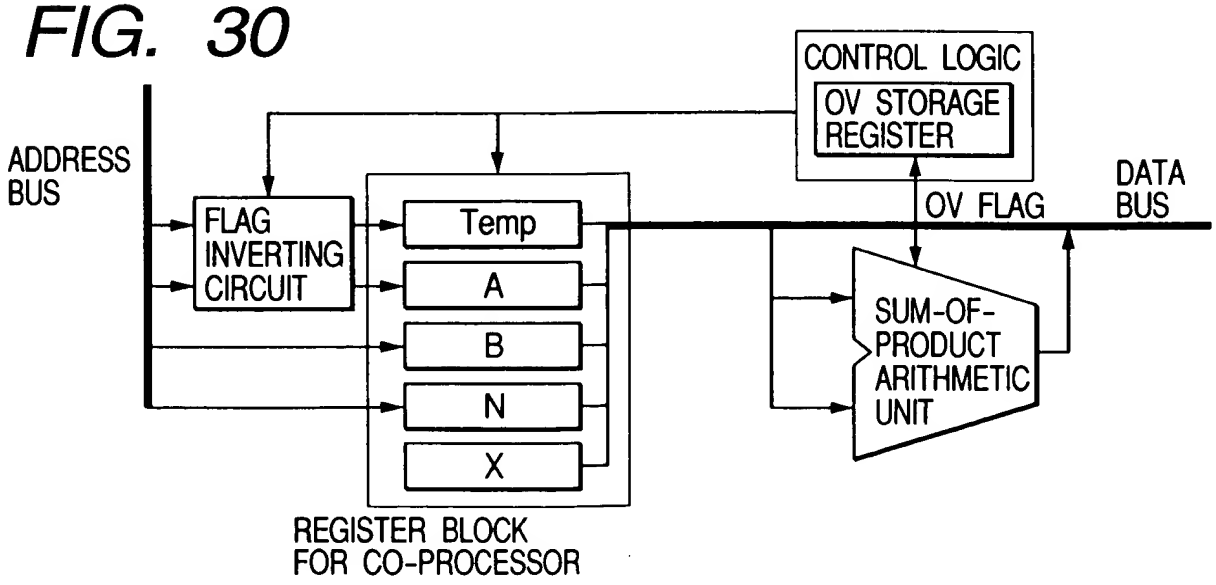



FIG. 30